Blumira Editions 2024

Blumira

The Value of Blumira's Free SIEM

Security monitoring for 3 cloud apps in minutes

Making Security Accessible to All

Help SMBs struggling w/security costs & complexity

- Affordable (free)
- Easy-to-deploy in minutes by existing team
- All-in-one - cloud SIEM, detection & response

Easiest, Fastest Time to Security

Avg SIEM setup often fails or takes weeks to months to get operational

- Cloud Connectors takes minutes for setup
- Logs imported & rules activated automatically
- Any IT admin can do it

Security Coverage For Microsoft 365 & More

M365 is commonly used by SMBs and targeted by attackers

- Key integration to start log collection & detection
- Expand to cover entire tech stack - on-prem & cloud*
- 24/7 support for urgent issues*

**Paid editions only*

Blumira

What You Get For Free

Security monitoring for 3 cloud apps – unlimited seats & data

- **Free cloud SIEM** for 3 cloud apps – choose from M365, Duo, SentinelOne, Webroot, Mimecast, Google Workspace, Sophos, JumpCloud, OneLogin
- **Easy, guided setup** through Cloud Connectors in minutes
- **Actionable findings** surfaced by Blumira's automated detection and response
- **Rule insight – see all active detection rules** automatically deployed
- **Detection rule management** to turn on/off rules to reduce noise
- **Managed detections** are maintained by our engineers
- **A summary dashboard** of your rules, connection status and security reports
- **1 week of log data retention** (upgrade for up to a year to meet compliance/insurance requirements)

Blumira

SIEM Starter

$15
Per seat/month

- Min 10 agents (1 seat)

Get everything in Free, plus:

- **Access to all cloud integrations** for greater coverage
- **Customer support** for urgent priority issues from 9am-8pm ET
- **White glove onboarding** with a dedicated Solution Architect, one-time fee required ($250)
- **Advanced reporting & dashboards** to see security trends & send scheduled reports. Includes pre-built compliance reports - upgrade to SIEM Starter + Compliance for Executive Summaries
- **90 days of data retention**, useful for investigation - upgrade to SIEM Starter + Compliance for one year of retention
- **Detection rule management & detection filters** to toggle rules on/off, or further customize to suit your organization's needs
- **50 max Blumira Agents** for endpoint visibility and response (min 10)
- **Manual host isolation** allows IT admins to contain (cut off from the network) affected endpoints manually through Blumira Agent

Purchase online, contracted on monthly basis

Blumira

SIEM+

$20
Per seat/month

- Min 50 agents (1 per seat)
- Additional agents $3 each/month

Get everything in SIEM Starter, plus:

- **Access to all cloud + sensor integrations** for complete coverage
- **24/7 Security Operations (SecOps) support** for urgent priority issues
- **White glove onboarding** with dedicated Solution Architect for one-time required fee ($500)
- **External threat surface scans** biannually
- **Dedicated CSM + recurring syncs** on a quarterly basis
- **1 year of data retention**, needed to meet most compliance and cyber insurance requirements
- **Blumira Investigate** for easy log searching & reports for investigation
- **Unlimited Blumira Agents** for endpoint visibility and response (min 50)
- **Manual host isolation** allows you to remotely isolate an affected endpoint to contain an identified threat
- **Manual dynamic blocklists** sends you an alert about known malicious sources of traffic, asking if you want to block the source & add to your blocklist
- **Honeypots** to gain visibility into active threats, like unauthorized access attempts within your environment

Blumira

XDR Platform

Get everything in SIEM+, plus:

- **1 year of data retention**, with longer term retention options
- **White glove onboarding** with a dedicated Solution Architect included with no additional fee
- **Automated host isolation** immediately isolates an affected endpoint to contain an identified threat when a finding is triggered (priority of finding is configurable)
- **Automated blocking (for dynamic blocklists)** immediately blocks access by known malicious traffic when a finding is triggered by your firewall, with no need for your team to review or respond to the finding

$25

Per seat/month

Min 50 agents (1 per seat)

Additional agents $3 each/month

Blumira